BLOCKCHAIN AND WEB3: FOUNDATIONS AND IMPLEMENTATION (PART 1)

Dirk Draheim

Friday 11 Nov 2022, 13:45
U06A-229, U06 Study Building
Ehitajate tee 5

TALLINN UNIVERSITY OF TECHNOLOGY

Outline

- Motivation
- Basics
  - Definitions: Peer-to-Peer Networks, Distributed Ledgers (DL), Blockchains, Consensus Problems in DLs / Blockchains
  - Blockchain Data Structures
  - Basic Understanding of Major Blockchain Consensus Mechanisms
- KSI Cash (feasibility study of the digital euro)
  - Today's Monetary System / Central Bank Digital Currency
  - KSI Cash Data Structures
  - KSI Performance Test
- Web3
  - History of the Web
  - The Web3 Vision
  - Towards Web35 Architectural Principles
- A Platform for Universal Asset Tokenization
- Conclusion

(Part 2)
25 Nov 2022

TAL TECH

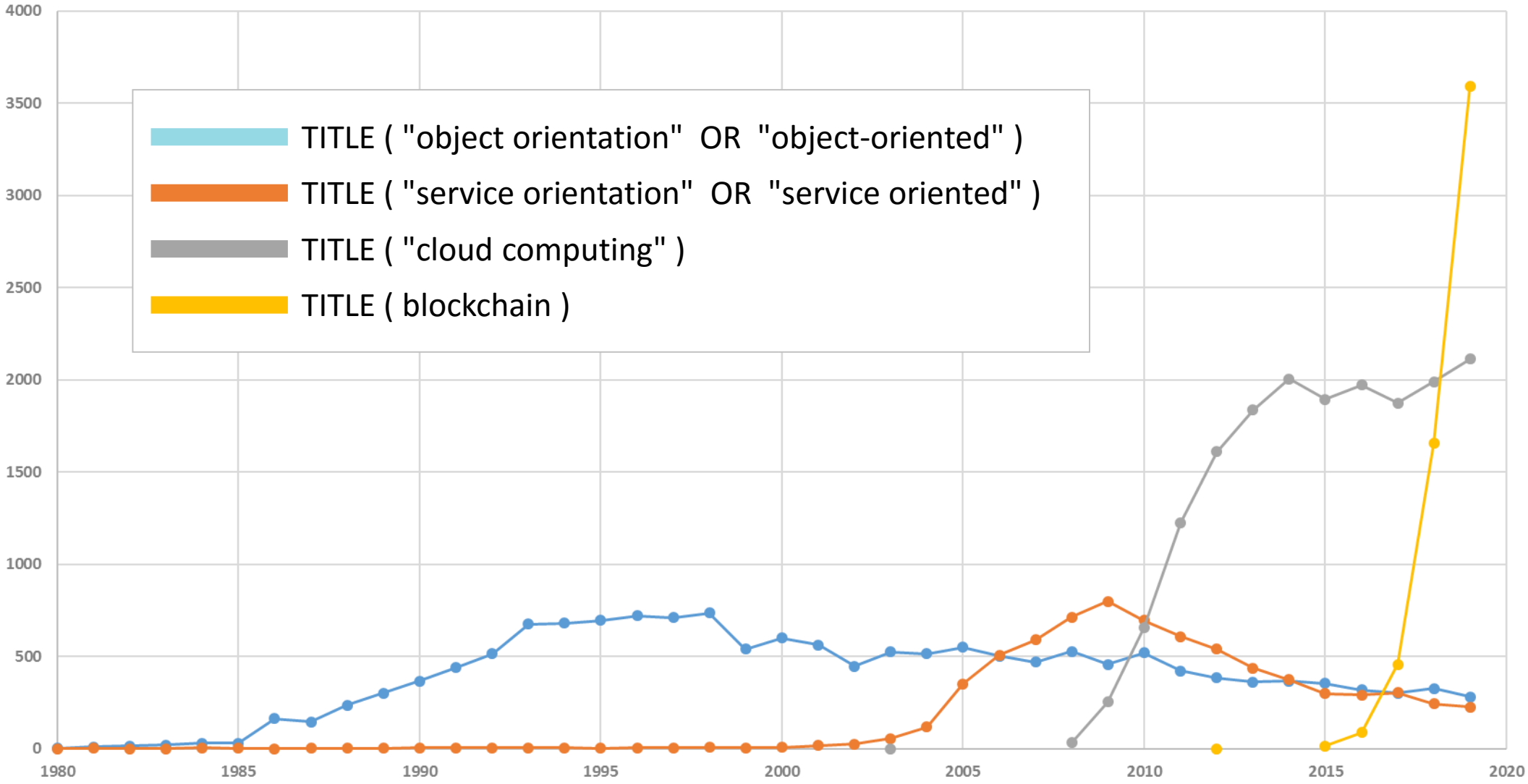
MOTIVATION

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

IT Paradigms and Research: Scopus Search (1980-2019)



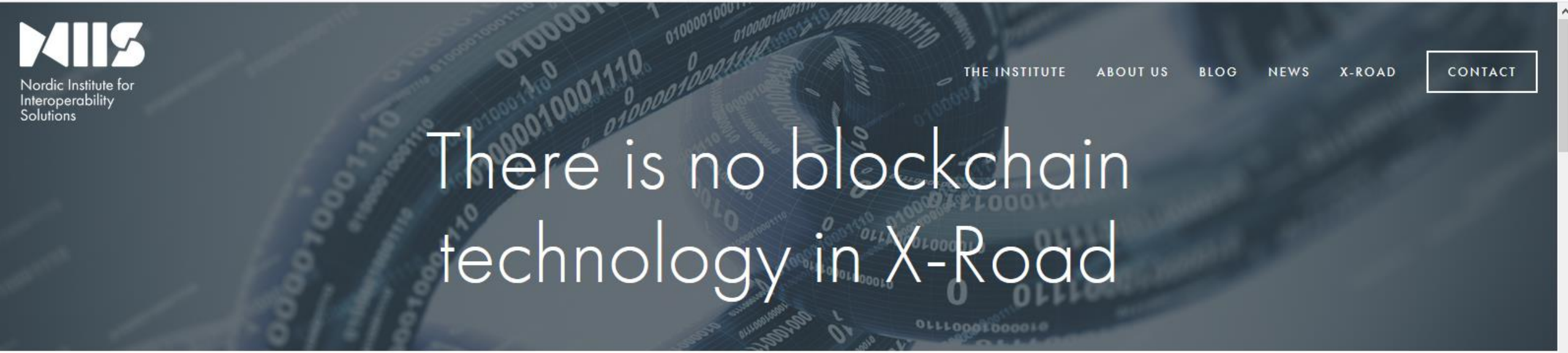
LETTER FROM TALLINN DECEMBER 18 & 25, 2017 ISSUE

ESTONIA, THE DIGITAL REPUBLIC

Its government is virtual, borderless, blockchained, and secure. Has this tiny post-Soviet nation found the way of the future?

By Nathan Heller

December 11, 2017



There is no blockchain technology in X-Road

Petteri Kivimäki · 26 April 2018

Recently there have been multiple writings about the X-Road which have stated that X-Road is a blockchain based technology or it utilizes blockchain internally. Are these claims true, is X-Road based on blockchain? Let's take a look at the facts.

Blockchain

Blockchain is one of this year's buzzwords and one of the hottest technologies out there. Blockchain

- ''To be clear, this [virtual currencies] is not about digital payments in existing currencies -- through Paypal and other `e-money' providers such as Alipay in China, or M-Pesa in Kenya. Virtual currencies are in a different category, because they provide their own unit of account and payment systems. These systems allow for peer-to-peer transactions without central clearinghouses, without central banks. For now, virtual currencies such as Bitcoin pose little or no challenge to the existing order of fiat currencies and central banks. Why? Because they are too volatile, too risky, too energy intensive, and because the underlying technologies are not yet scalable. Many are too opaque for regulators; and some have been hacked. But many of these are technological challenges that could be addressed over time. Not so long ago, some experts argued that personal computers would never be adopted, and that tablets would only be used as expensive coffee trays. So I think it may not be wise to dismiss virtual currencies.''

TAL TECH

Chrisine Lagarde: Central banking and Fintech – A brave new world? Bank of England Conference, London, 29 September (2017)

Web3

- „ Web3 Is Our Chance to Make a Better Internet.“ (Jin, Parrott, 2022)
- „The Web3 movement seeks to liberate us from Big Tech and exploitative capitalism – and to do it using only blockchain, game theory, and code.“ (Edelman, 2022)

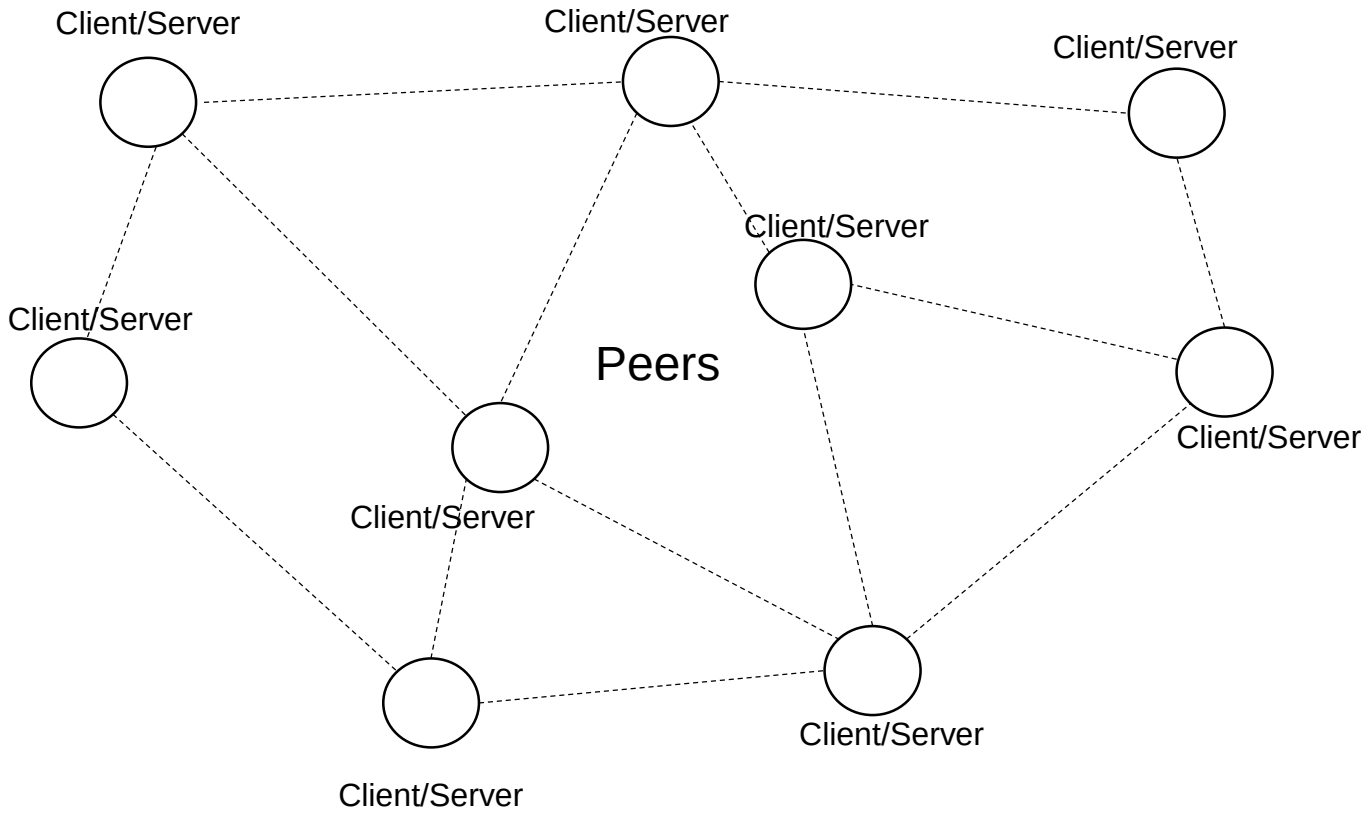
- Li Jin and Katie Parrott. Web3 Is Our Chance to Make a Better Internet. Harvard Business Review, 10 May 2022.
- Jad Esber and Scott Duke Kominers. Why Build in Web3. Harvard Business Review 16 May 2022.

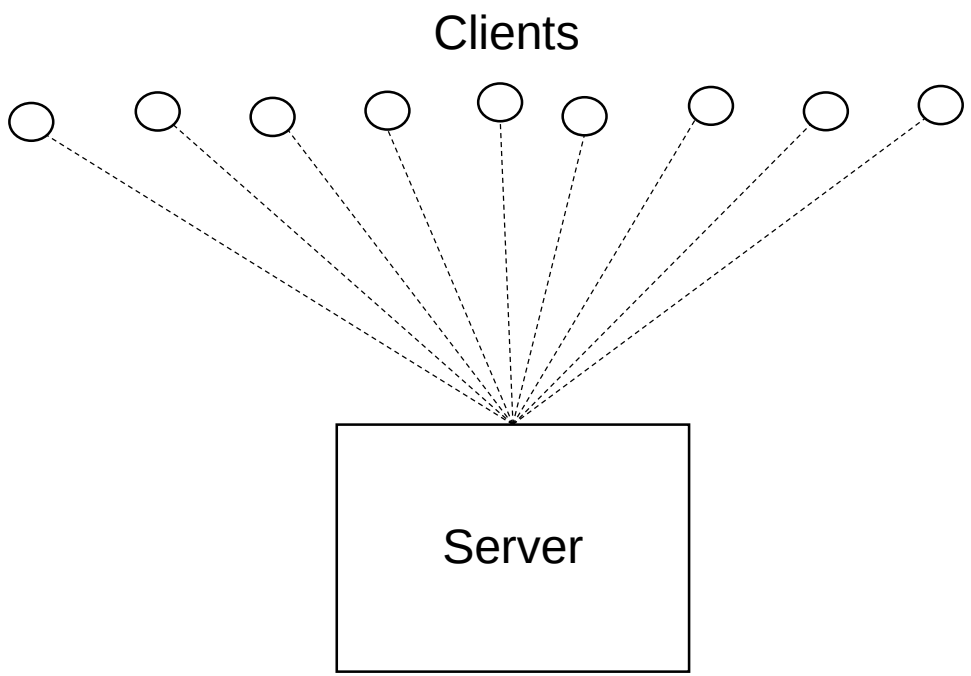
BASICS

Definitions

- **Peer-to-Peer (P2P) Network**: distributed application model in which nodes are clients and servers at the same time; nodes are equal partners that cooperate to achieve a common goal
- **Distributed Ledger (DL):** database that is replicated over all nodes of a peer-to-peer network.
- **Blockchain (narrow sense):** DL (of transactions) + algorithms (validation, consensus)+ P2P network that follows the original Bitcoin blockchain paradigm+design: cryptocurrency, permissionless (entry of new nodes is not restricted), organized in blocks that are linked by hashes; PoW consensus
- **Blockchain (wide sense):** all kinds of other data structures that show some (which?) of the characteristics of the ``blockchain in the narrow sense''. (this is pretty much a non-definition….)
- **Consensus**: state, in which all nodes of a blockchain have agreed on the same, validated database (validated wrt: basic consistency + commonly agreed-upon business rules)
- **Consensus Mechanism:** fault-tolerant process through which the nodes of a blockchain network achieve consensus; (core idea is always: by determining a publisher)
- **Publisher**: node that is determined to assemble and validate a block. (in PoW: called miner!; in PoV: leader); CORE challenge: we cannot trust any potential publisher; potential publishers might fail/cheat/attack!

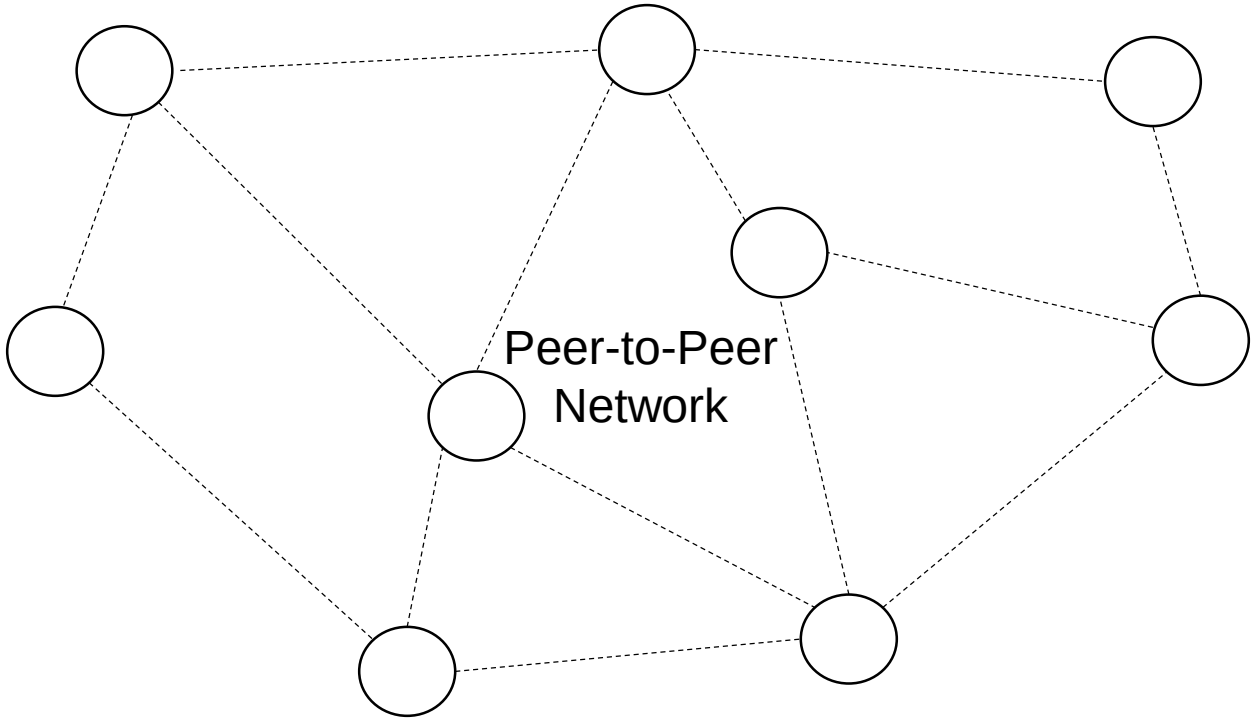
Peer-to-Peer Network





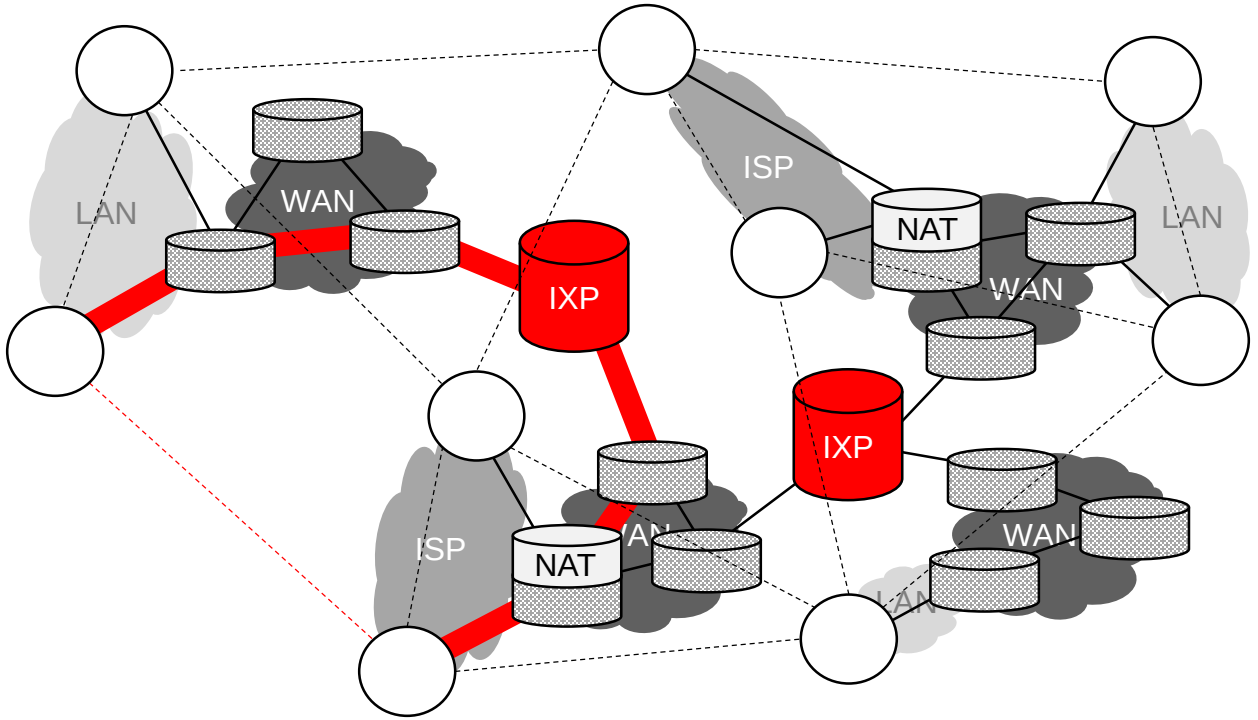
TAL TECH

Characteristic Neglection of the Physical Network

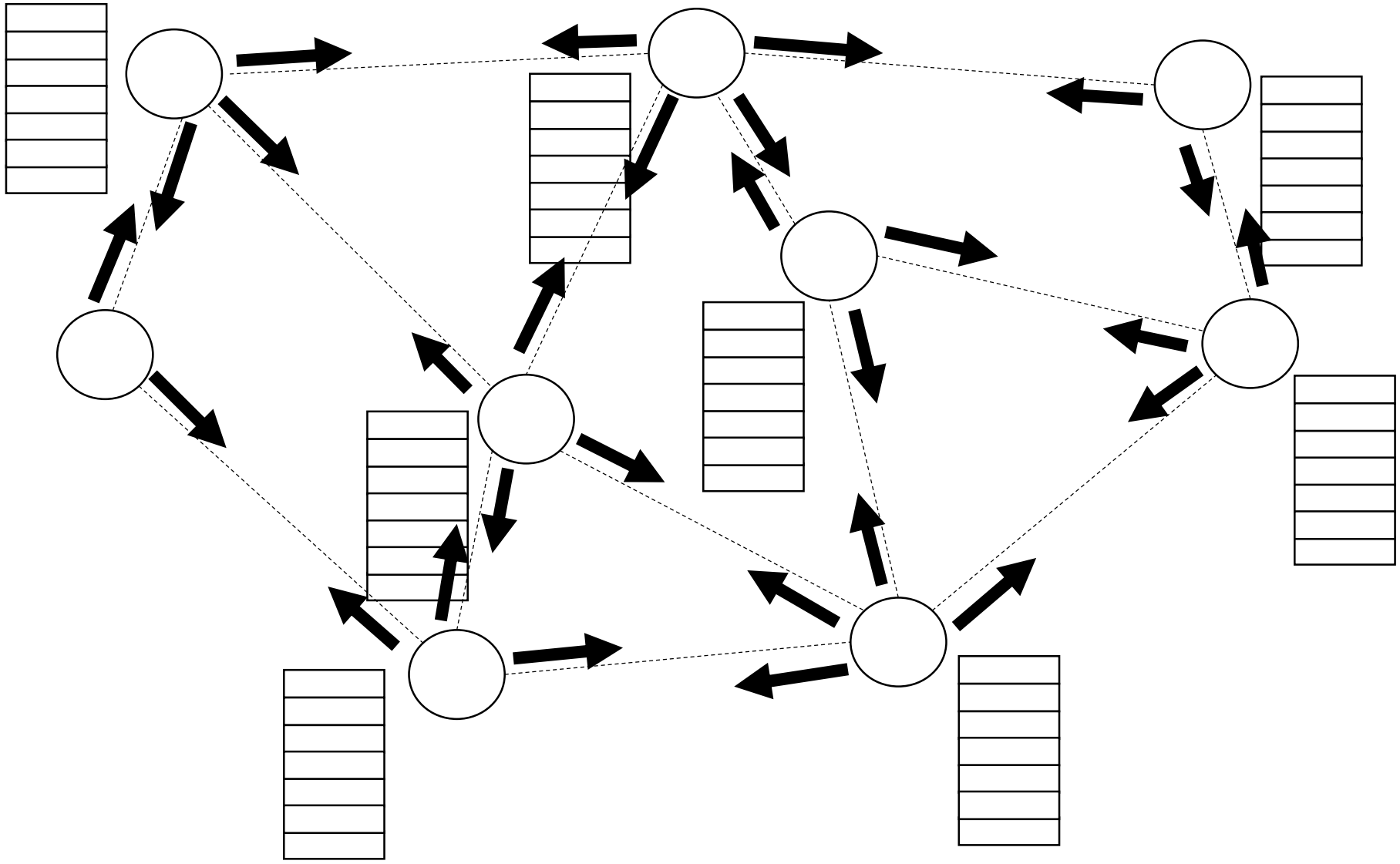


TAL TECH

Characteristic Neglection of the Physical Network

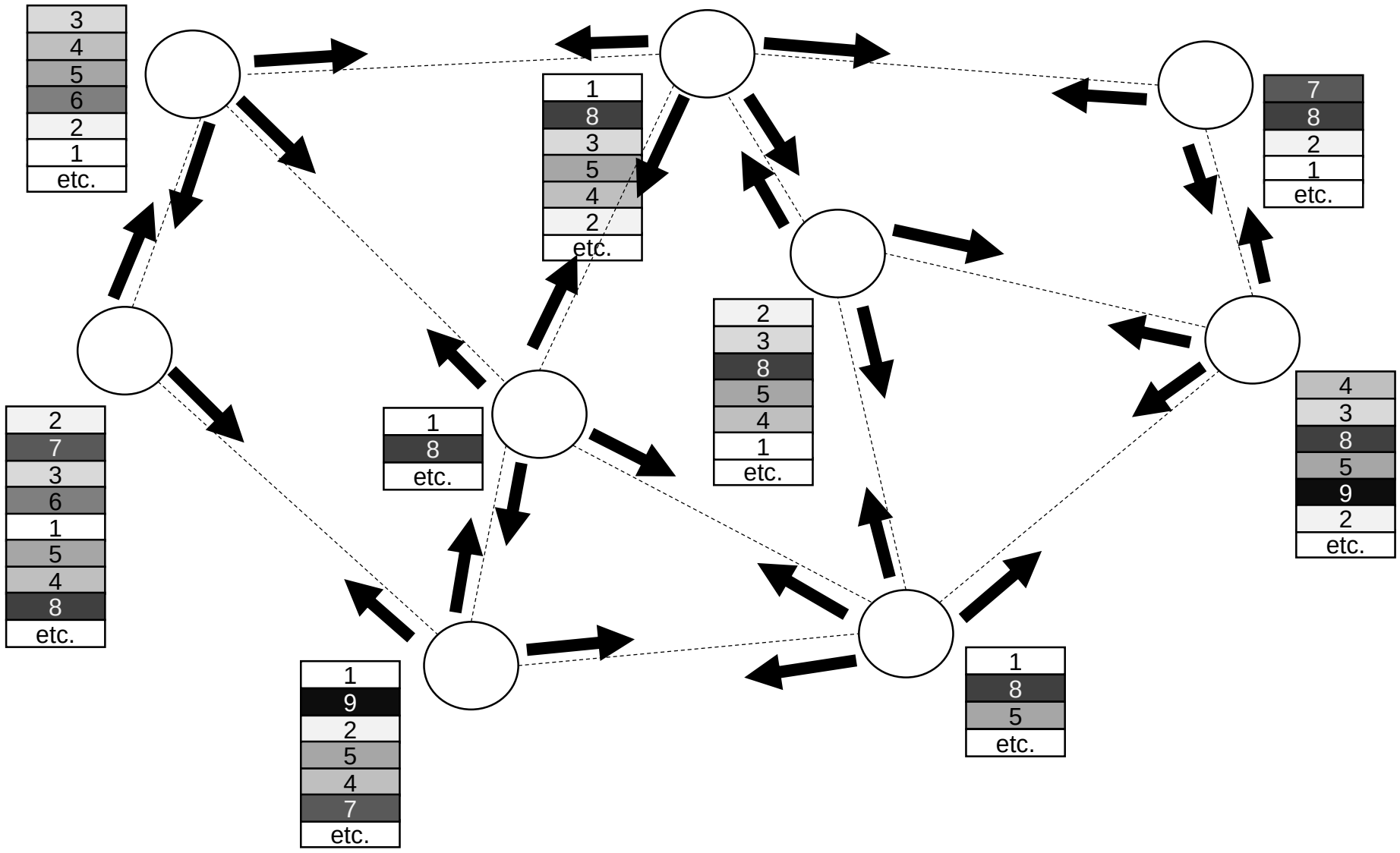


Distributed Ledger



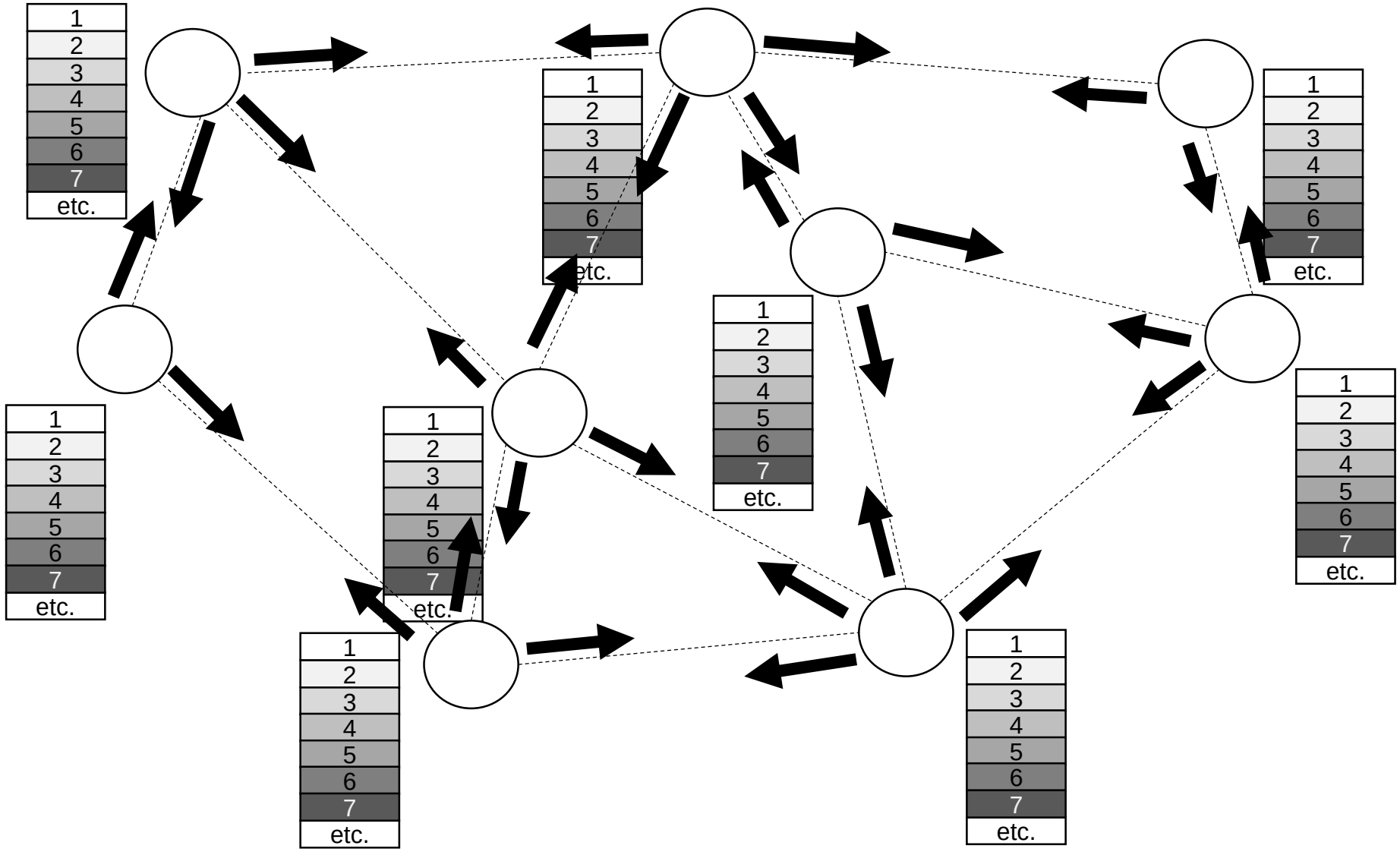
TAL TECH

Non-Consensual Chaos



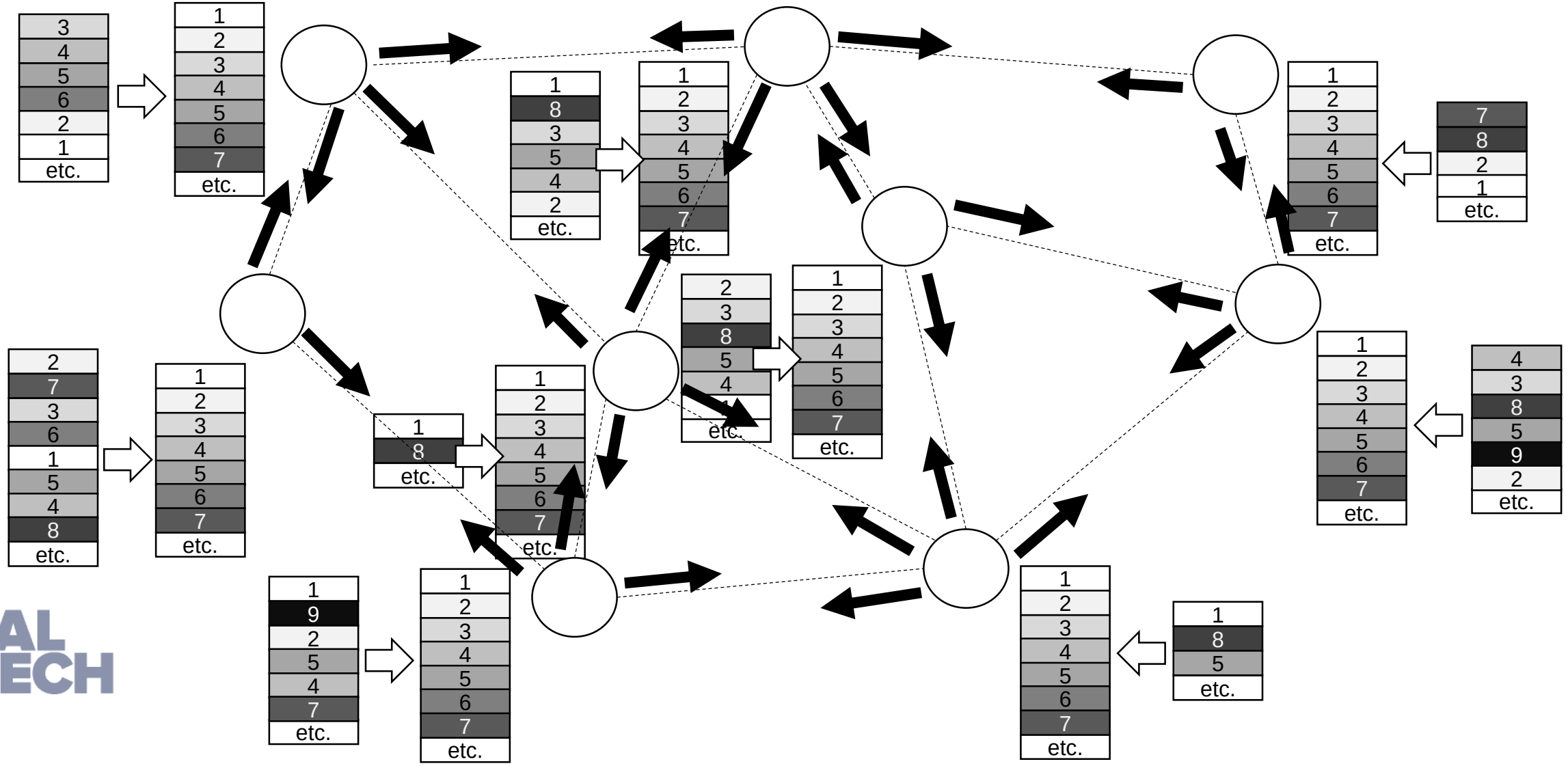
TAL TECH

Consensus



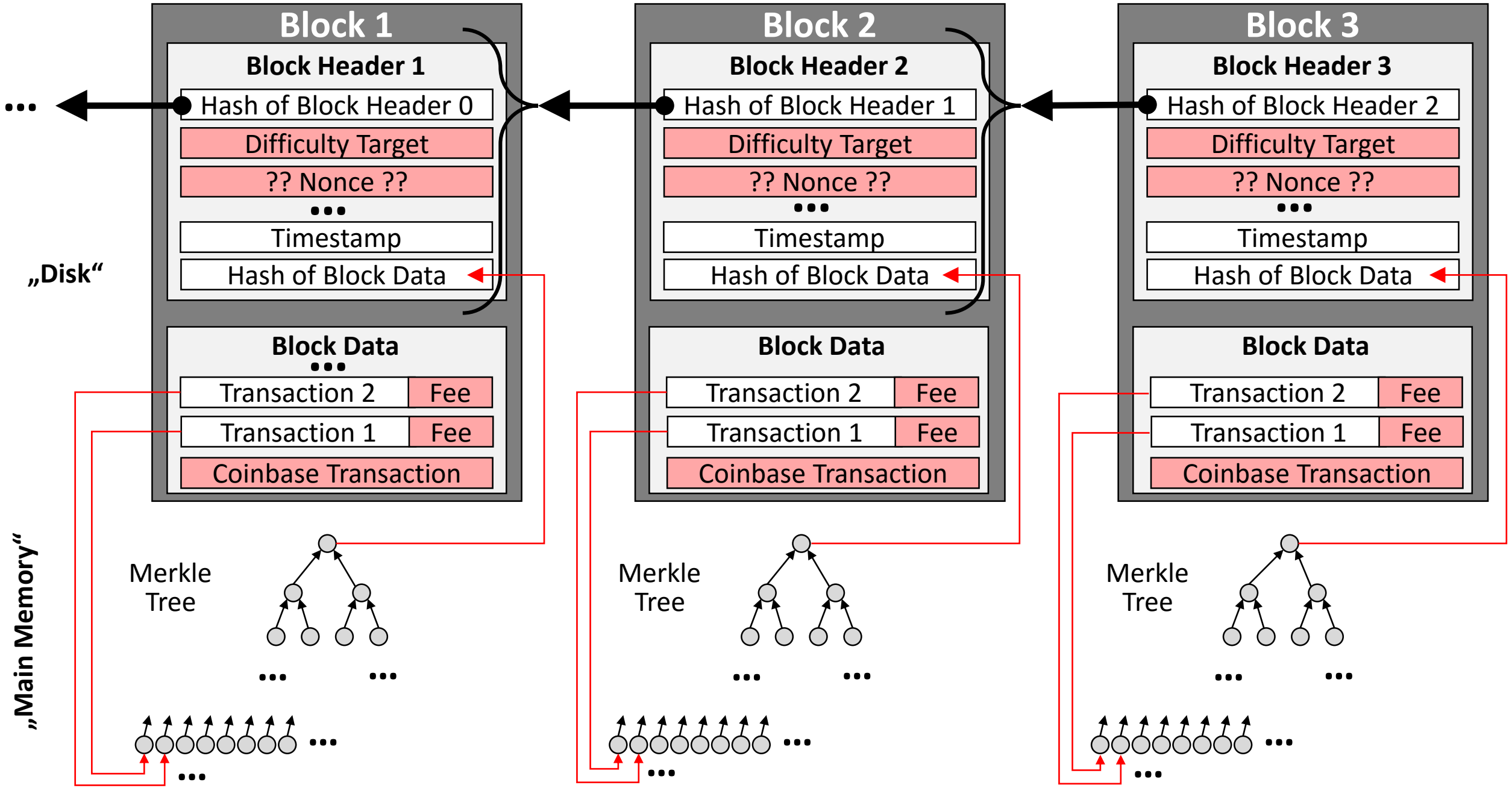
TAL TECH

Consensus Mechanism

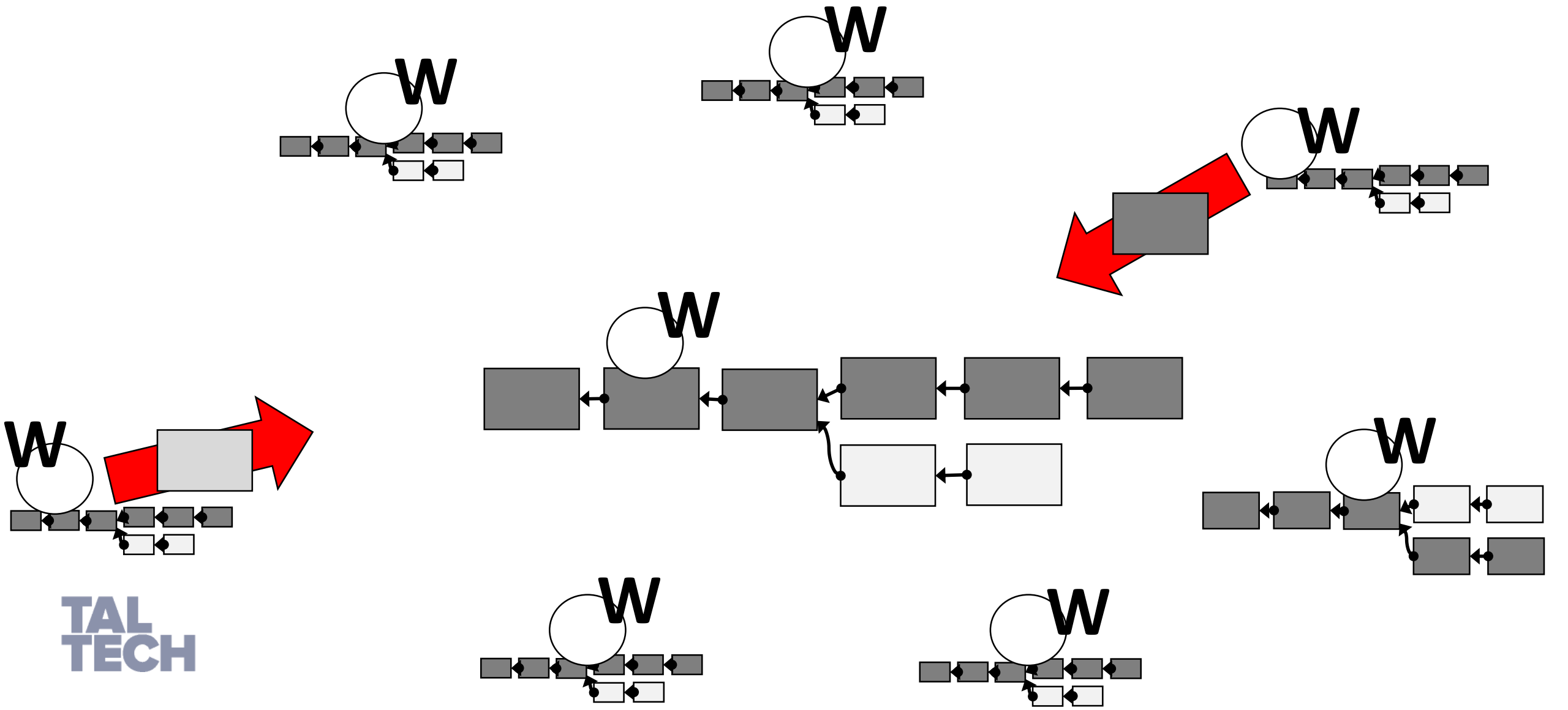


TAL TECH

Blockchain Data Structures (PoW)



Proof-of-Work



TAL TECH

Author | Topic: Proof of stake instead of proof of work (Read 32047 times)

QuantumMechanic
Member

Activity: 110
Merit: 16

Proof of stake instead of proof of work
July 11, 2011, 04:12:45 AM
Merited by Vod (2), webtricks (2), d5000 (1), drays (1)
#1

I've got an idea, and I'm wondering if it's been discussed/ripped apart here yet:

I'm wondering if as bitcoins become more widely distributed, whether a transition from a proof of work based system to a proof of stake one might happen. What I mean by proof of stake is that instead of your "vote" on the accepted transaction history being weighted by the share of computing resources you bring to the network, it's weighted by the number of bitcoins you can prove you own, using your private keys.

For those that don't want to be actively verifying transactions, and so that not all private keys need to be facing the network, votes could be delegated to other addresses via some kind of nonstandard Bitcoin transaction. In this way, voting power would accumulate with trusted delegates instead of miners. New bitcoins and transaction fees could be randomly and periodically distributed to delgates, weighted by the number of votes they've accumulated, thereby incentivising diversity of the delegates and direct voters.

If the implementation could be done, it proved to maintain at least a similar level of privacy and trustworthiness, and it only minimally complicated the UX, I'm thinking that a proof of stake based fork could out-compete a proof of work one due to much lower transaction fees, since its network wouldn't need to support the cost of the miners' computing resources. (Note that the vote delegation scheme has bandwith/storage overhead that would offset these savings by some amount which would hopefully be relatively small.)

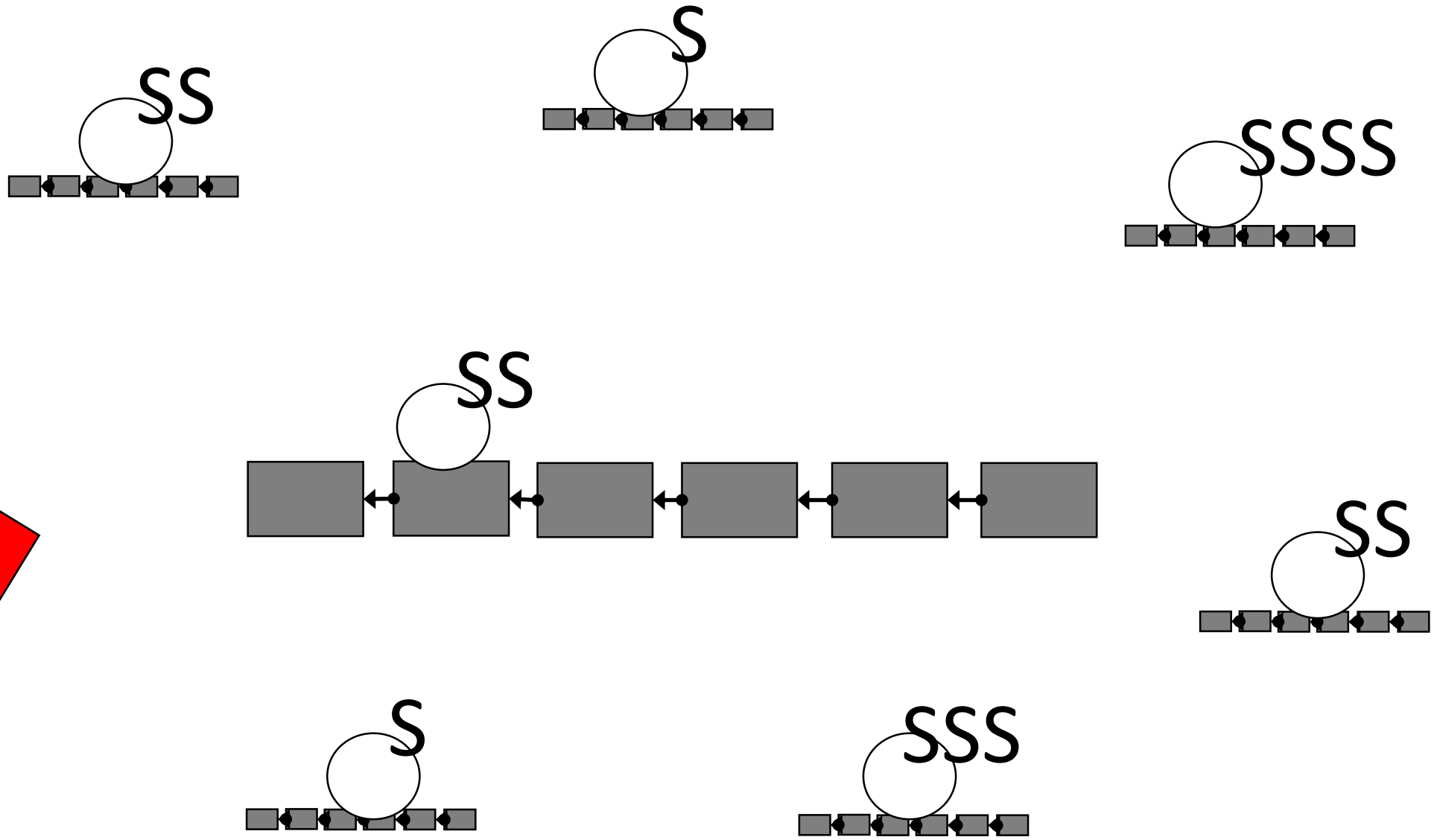
Some other potential improvements this system could offer:

- Possibly quicker, more definite confirmation of transactions, depending on how it can be implemented.
- The "voting power" may be more trustworty, since it would accumulate in a bottom-up fashion via a network of trust, instead of in the somewhat arbitrary way it accumulates now. (Note the potential problem of vote-buying here.)
- It would remove the physical point of failure of bitcoin mining equipment, which can be confiscated or made illegal to run.
- It could be used to provide stakeholders a means of making their voices heard (via the delegated voting system it establishes) when it comes to proposals for software updates and protocol changes.

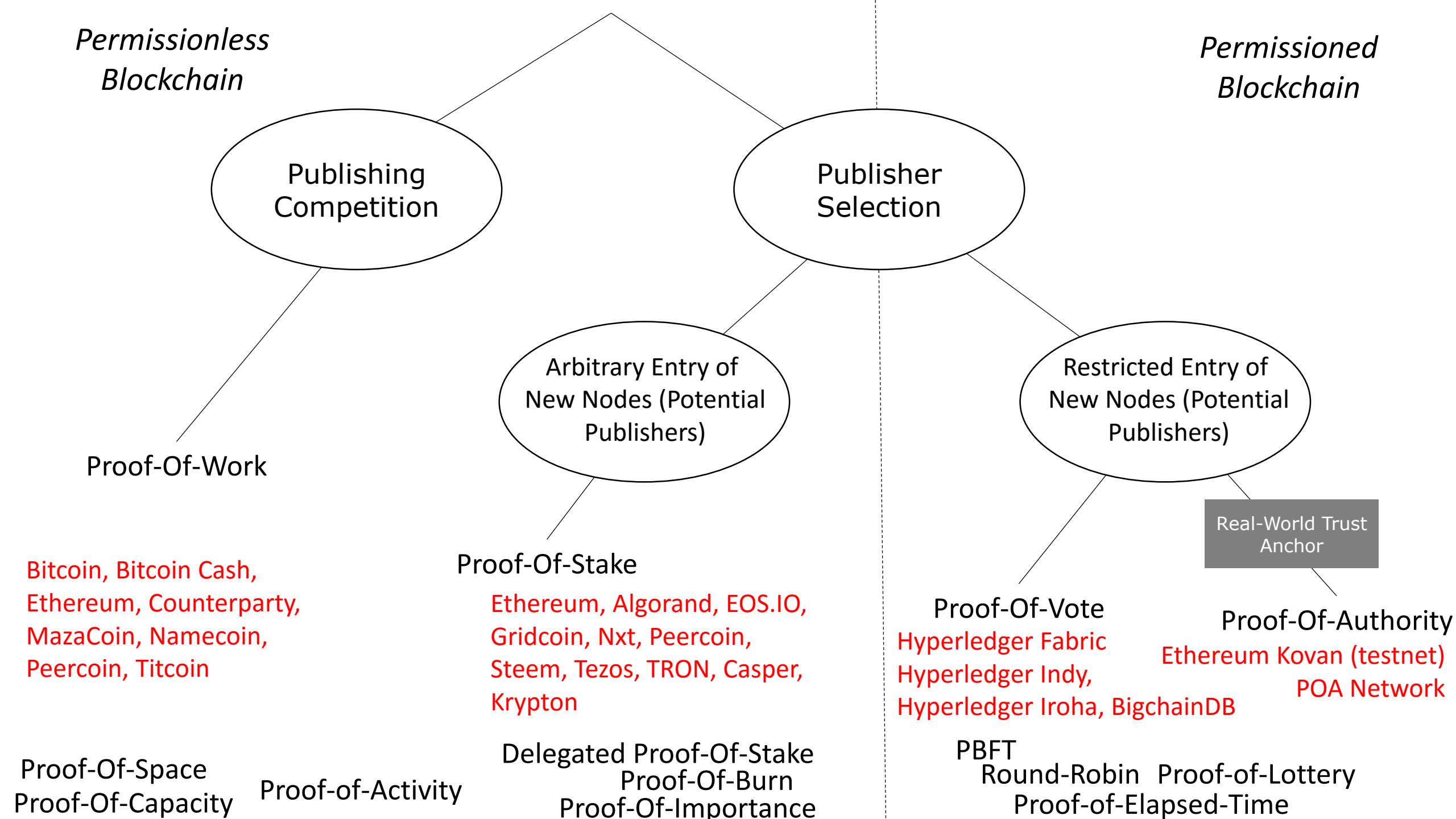
Anyway, I just wanted to throw the idea out here to see if there are any obvious reasons why it couldn't be implemented, and to hopefully spark a discussion amongst those better qualified than me.

Cheers.

Proof-of-Stake



TAL TECH


Permissionless Blockchain
Permissioned Blockchain
Publishing Competition
Publisher Selection
Arbitrary Entry of New Nodes (Potential Publishers)
Restricted Entry of New Nodes (Potential Publishers)
Real-World Trust Anchor
Proof-Of-Work
Bitcoin, Bitcoin Cash, Ethereum, Counterparty, MazaCoin, Namecoin, Peercoin, Titcoin
Proof-Of-Stake
Ethereum, Algorand, EOS.IO, Gridcoin, Nxt, Peercoin, Steem, Tezos, TRON, Casper, Krypton
Proof-Of-Vote
Hyperledger Fabric Hyperledger Indy, Hyperledger Iroha, BigchainDB
Proof-Of-Authority
Ethereum Kovan (testnet) POA Network
Proof-Of-Space
Proof-Of-Capacity
Proof-of-Activity
Delegated Proof-Of-Stake
Proof-Of-Burn
Proof-Of-Importance
PBFT
Round-Robin
Proof-of-Lottery
Proof-of-Elapsed-Time

Further Readings

- Dylan Yaga, Peter Mell, Nik Roby, Karen Scarfone. Blockchain Technology Overview. Techn. Report No. NISTIR 8202, National Institute of Standards and Technology, 2018. https://doi.org/10.6028/NIST.IR.8202
- Andreas M. Antonopoulos. Mastering Bitcoin: Programming the Open Blockchain. O'Reilly, 2017.
- Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf
- Jing Chen, Sergey Gorbunov , Silvio Micali, Georgios Vlachos. Algorand Agreement: Super Fast and Partition Resilient Byzantine Agreement. Techn. Report No. 20180501:150853, Algorand Foundation, 2018. https://eprint.iacr.org/2018/377
- Vita Krainik. Distributed Consensus Problems and Protocols: a Systematic Literature Review . Master’s Thesis. Tallinn University of Technology, 2019. https://digikogu.taltech.ee/en/Item/6060be75-8225-4880-8947-57168c3d3c44

TAL TECH

Conclusion

- **Peer-to-Peer (P2P) Network**: distributed application model in which nodes are clients and servers at the same time; nodes are equal partners that cooperate to achieve a common goal
- **Distributed Ledger (DL):** database that is replicated over all nodes of a peer-to-peer network.
- **Blockchain (narrow sense):** DL (of transactions) + algorithms (validation, consensus)+ P2P network that follows the original Bitcoin blockchain paradigm+design: cryptocurrency, permissionless (entry of new nodes is not restricted), organized in blocks that are linked by hashes; PoW consensus
- **Blockchain (wide sense):** all kinds of other data structures that show some (which?) of the characteristics of the ``blockchain in the narrow sense''. (this is pretty much a non-definition….)
- **Consensus**: state, in which all nodes of a blockchain have agreed on the same, validated database (validated wrt: basic consistency + commonly agreed-upon business rules)
- **Consensus Mechanism:** fault-tolerant process through which the nodes of a blockchain network achieve consensus; (core idea is always: by determining a publisher)
- **Publisher**: node that is determined to assemble and validate a block. (in PoW: called miner!; in PoV: leader); CORE challenge: we cannot trust any potential publisher; potential publishers might fail/cheat/attack!